

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

BROWSERKEY, LLC,

Plaintiff,

v.

ALLY FINANCIAL, INC.

Defendant.

§
§
§
§
§
§
§
§
§
§

Case No.

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff BrowserKey, LLC (“BrowserKey” or “Plaintiff”) for its Complaint against Ally Financial, Inc. (“Ally Financial” or “Defendant”) alleges as follows:

THE PARTIES

1. BrowserKey is incorporated under the laws of the State of Texas, with a place of business located at 101 East Park Boulevard, Suite 600, Plano, Texas 75074.

2. Upon information and belief, Defendant Ally Financial is a corporation organized and existing under the laws of the State of Delaware, with a place of business at 500 Woodward Avenue, Detroit, Michigan 48226, and with additional regular and established places of business in this District at least at 2911 Lake Vista Drive, Lewisville, Texas 75067. Upon information and belief, Defendant may be served with process via its registered agent, The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801.

JURISDICTION AND VENUE

3. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq.* This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331, 1332, 1338, and 1367.

4. This Court has specific and personal jurisdiction over Defendant consistent with the requirements of the Due Process Clause of the United States Constitution and the Texas Long Arm Statute. Upon information and belief, Defendant has sufficient minimum contacts with the forum because Defendant has physical locations and transacts substantial business in the State of Texas and in this Judicial District. Further, Defendant has, directly or through subsidiaries or intermediaries, committed acts of patent infringement in the State of Texas and in this Judicial District as alleged in this Complaint, as alleged more particularly below.

5. Venue is proper in this Judicial District pursuant to 28 U.S.C. §§ 1391 and 1400(b). Defendant is registered to do business in Texas and, upon information and belief, Defendant has transacted business in this Judicial District, has committed acts of direct and indirect infringement in this Judicial District, and has regular and established places of business in this Judicial District as set forth above. Defendant is subject to personal jurisdiction in this Judicial District and has committed acts of patent infringement in this Judicial District. On information and belief, Defendant through its own acts and/or through the acts of others, makes, uses, sells, offers to sell, and/or imports infringing products within this Judicial District, regularly does and solicits business in this Judicial District, and has the requisite minimum contacts with the Judicial District, such that this venue is a fair and reasonable one.

U.S. PATENT NO. 7,249,262

6. On July 24, 2007, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,249,262 (the “’262 Patent,” or “Patent-in-Suit”) entitled “Method For Restricting Access To A Web Site By Remote Users.” A true and correct copy of the ’262 Patent is attached hereto as Exhibit A.

7. BrowserKey is the sole and exclusive owner of all right, title, and interest to and in the ’262 Patent, and holds the exclusive right to take all actions necessary to enforce its rights to the ’262 Patent, including the filing of this patent infringement lawsuit. BrowserKey also has the right to recover all damages for infringement of the ’262 Patent as appropriate under the law.

INFRINGEMENT ALLEGATIONS

8. The ’262 Patent generally covers a method of restricting access to data maintained on a server computer by one or more authorized, networked client machines. The technology was developed by Leon E. Hauck and Brent J. Burval. This technique is incorporated into web and mobile applications made by numerous banking institutions, including Ally Financial.

9. Ally Financial has manufactured, used, marketed, distributed, sold, offered for sale, exported from, and imported into the United States, products that infringe the ’262 Patent. These Accused Products include at least all versions and variants of the Ally Financial Web and Mobile Applications since 2019. The Accused Products include at least all versions and variants of the Ally Financial Mobile Applications which have supported any biometric, token-based, and/or passwordless authentication. For example, the Accused Products comprise at least the Ally: Bank, Auto & Invest (a.k.a. Ally Financial App, Ally Financial Mobile Application, or Ally Financial Mobile App) for iOS, iPad, and Android, including all supporting servers, computer systems, and infrastructures, since at least 2019.

10. BrowserKey has at all times complied with the marking provisions of 35 U.S.C. § 287 with respect to the '262 Patent.

11. Upon information and belief, Ally Financial has had knowledge and notice of the Patent-in-Suit, and its infringement thereof, since they were issued. Ally Financial, as a bank, regularly monitors ways to secure their mobile and web application, and upon information and belief, monitored or was otherwise aware of Plaintiff's patented inventions, including due to their impact on Ally Financial and Ally Financial's competitor's security systems. Alternatively, to the extent that Ally Financial avoided actual knowledge of the Patent-in-Suit, and its infringement thereof, it was willfully blind. Upon information and belief, to the extent it lacked actual knowledge of infringement, Ally Financial deliberately avoided learning of infringement, despite subjectively believing that there was a high probability that it infringed Plaintiff's patents, and specifically the Patent-in-Suit. Upon information and belief, Ally Financial has adopted a policy or practice of not reviewing the patents of others, including those related to Ally Financial's specific industry and of Plaintiff in particular, thereby remaining willfully blind to the Patent-in-Suit. Upon information and belief, Ally Financial lacks written policies disseminated to employees regarding monitoring or avoidance of patent infringement by Ally Financial and lacks mechanisms for employees to report patents which they believe Ally Financial may infringe. Upon information and belief, Ally Financial and its employees understood that there was a high likelihood that patents filed on innovations by Plaintiff read on the Accused Products.

COUNT I
(Infringement of the '262 Patent)














12. Paragraphs 1 through 11 are incorporated by reference as if fully set forth herein.

13. BrowserKey has not licensed or otherwise authorized Ally Financial to make, use, offer for sale, sell, or import any products that embody the inventions of the '262 Patent.

14. Ally Financial has and continues to directly infringe the '262 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '262 Patent. These products include at least all versions and variants of the Ally Financial Web and Mobile Applications.

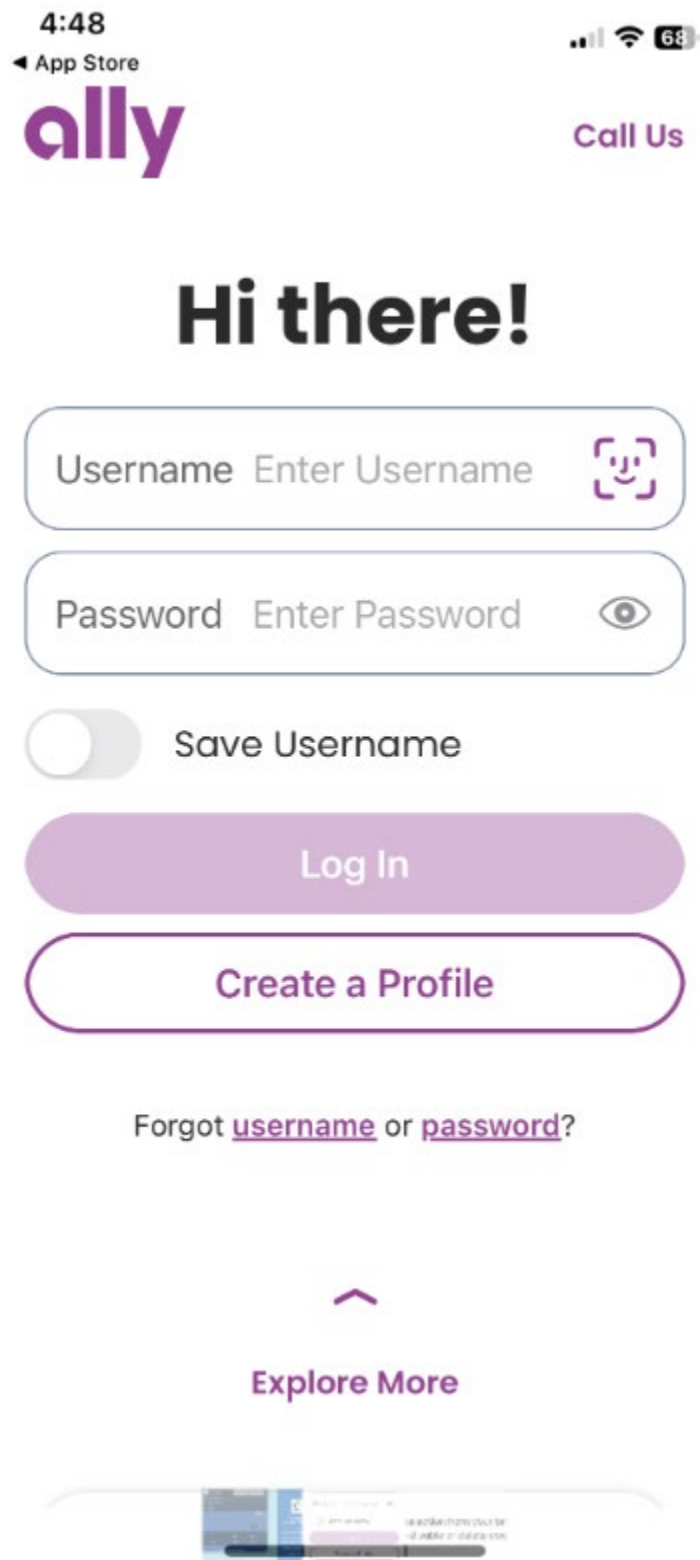
15. For example, Ally Financial directly infringes at least claim 1 of the '262 Patent by making, using, offering to sell, selling, and/or importing into the United States products that practice a method of restricting access to data maintained on a server computer by an authorized client machine, said method comprising the steps of: a. installing a client-side software program on the client machine for generating a client machine-specific identifier, the client machine-specific identifier being substantially unique to the particular machine upon which such client-side software program is initially installed; b. operating the client-side software program on the client machine to generate the client machine-specific identifier; c. generating a password remote from the client machine and providing the password to a user of the client machine, the password being derived from the client machine-specific identifier generated in step b., and uniquely corresponding thereto; d. issuing a request by the client machine to the server computer for access to data maintained on the server computer; e. responding to the request for access of step d. by having the client machine re-generate its machine-specific identifier; f. verifying on the client machine whether the client machine-specific identifier re-generated in step e. uniquely corresponds with the password generated in step c.; and g. recognizing the client machine as being authorized to access data maintained on the server computer if the verification performed by step f. is true, and refusing to recognize the client machine as being authorized to access data maintained on the server computer if the verification performed by step f. is false.

16. The Accused Products practice a method of restricting access to data maintained on a server computer by an authorized client machine. For example, upon information and belief, on client machines running the Ally Financial Mobile Application variant for Apple iOS, one method by which an operator may sign in to access Ally Financial's "protected URLs," as an Ally Financial account holder, is via Apple's Touch and Face ID (locally compared "biometrics"). This biometric process authorizes the client machine to access restricted data on Ally Financial server(s).

Phones  	
Products & Rates	
Transfers	
Ally eCheck Deposit SM	
Savings Buckets & Boosters	
Spending Buckets	
Bill Pay	
Zelle [*]	
CD Management	
ATM Locator	
Ally Assist	
Biometric Verification (Optional)	

1

¹ <https://www.ally.com/bank/online-banking/>



2

² Screen shot of Ally Mobile Banking Application

17. The Accused Products further practice a method of installing a client-side software program on the client machine for generating a client machine-specific identifier, the client machine-specific identifier being substantially unique to the particular machine upon which such client-side software program is initially installed. For example, a client-side software program (e.g., the Ally Financial Mobile Application) is installed on the client machine (e.g., a phone running Ally Financial's Mobil Application), and generates a client machine specific identifier (e.g., a device key, certificate, public/private key pair, and/or other cryptographic material). Upon information and belief, each such identifier is unique to the client machine upon which such client-side software program is initially installed (e.g., to an instance of Ally Financial's Mobile Application running on a specific client machine).

18. The Accused Products further practice a method of operating the client-side software program on the client machine to generate the client machine-specific identifier. For example, upon launch of the Ally Financial Application, the Ally Financial servers verify that a client application adapted to calculate a machine specific identifier with a machine specific key (e.g., a Ally Financial Application configured to calculate a signature, device key, certificate, public/private key pair, and/or other cryptographic material based on cryptographic and/or seed material of a machine-specific identifier provided to the client by the server within a policy or registration request) exists on the client device (e.g., is installed), or provides that client application to the device (e.g., by triggering an update or transmission to the Ally Financial Application).

19. The Accused Products further practice a method of generating a password remote from the client machine and providing the password to a user of the client machine, the password being derived from the client machine-specific identifier generated in step b, and uniquely corresponding thereto. For example, upon information and belief, the Ally Financial servers

generate a password (e.g., a nonce, token, cryptographic key, certificate, cryptogram, signed nonce, and/or other cryptographic material) derived from a client machine-specific identifier generated on the client machine (e.g., by applying a signature or transform based on a seed value to a private key and/or device keys associated with, and/or generated based on material from, the secure element of the device). The Ally Financial servers then provide that password to the client machine (e.g., by transmitting the password to a smartphone running the Ally Financial Application via HTTP protocol). For example, upon information and belief, that password, is either stored inside, or wrapped in encryption provided by, a secure element/secure enclave/secure execution environment of the mobile device running the Ally Financial Application. Upon information and belief, the seed value, signature, and/or algorithm are also stored inside or wrapped in encryption provided by that secure element/secure enclave/secure execution environment.

20. The Accused Products further practice a method of issuing a request by the client machine to the server computer for access to data maintained on the server computer. For example, Ally Financial servers receive a request (e.g., an HTTP request) from a client machine (e.g., a smartphone running the Ally Financial Mobile Application) for access to data stored on a server (e.g., account information stored on a server) when the application is launched. For example, when first launching the Ally Financial Mobile Application, upon information and belief, a user agent requests a protected URL associated with Ally Financial.

21. The Accused Products further practice a method of responding to the request for access of step d. by having the client machine re-generate its machine-specific identifier, and verifying on the client machine whether the client machine-specific identifier re-generated in step e. uniquely corresponds with the password generated in step c. For example, upon information and



belief, when biometric authentication is enabled on the Ally Financial Mobile Application, the Ally Financial servers transmit instructions to re-generate the password (e.g., the seed value and algorithm that can be applied to the nonce, token, device key, public key, and/or key pair to generate a matching password and/or signed nonce), and to verify, on the client machine, whether the client machine-specific identifier uniquely corresponds with the password generated at step b (e.g., by utilizing fingerprint, face, or iris recognition to authenticate a user, thereby granting access to the secure element-protected password, and applying same to the seed value and algorithm to the public key, nonce, signature, and/or key pair to verify that it matches the one transmitted by the server). For example, upon information and belief, when the client machine supports Apple Touch / Face ID, and the Ally Financial Mobile Application has been provisioned to sign in to Ally Financial online services via Touch / Face ID, Ally Financial computer code automatically prompts the operator to sign in via Touch / Face ID immediately after the app is launched.

22. The Accused Products further practice a method of recognizing the client machine as being authorized to access data maintained on the server computer if the verification performed by step f. is true, and refusing to recognize the client machine as being authorized to access data maintained on the server computer if the verification performed by step f. is false. For example, if the sign in on the client machine is successful, access to data maintained on Ally Financial servers(s) is authorized by Ally Financial. If the client machine is not signed in, access to data maintained on Ally Financial servers(s) is denied by Ally Financial.

23. For example, Ally Financial directly infringes at least claim 11 of the '262 Patent by making, using, offering to sell, selling, and/or importing into the United States products that practice a method of restricting access to data maintained on a server computer by an authorized client machine, said method comprising the steps of: a. creating a session identifier in a computer

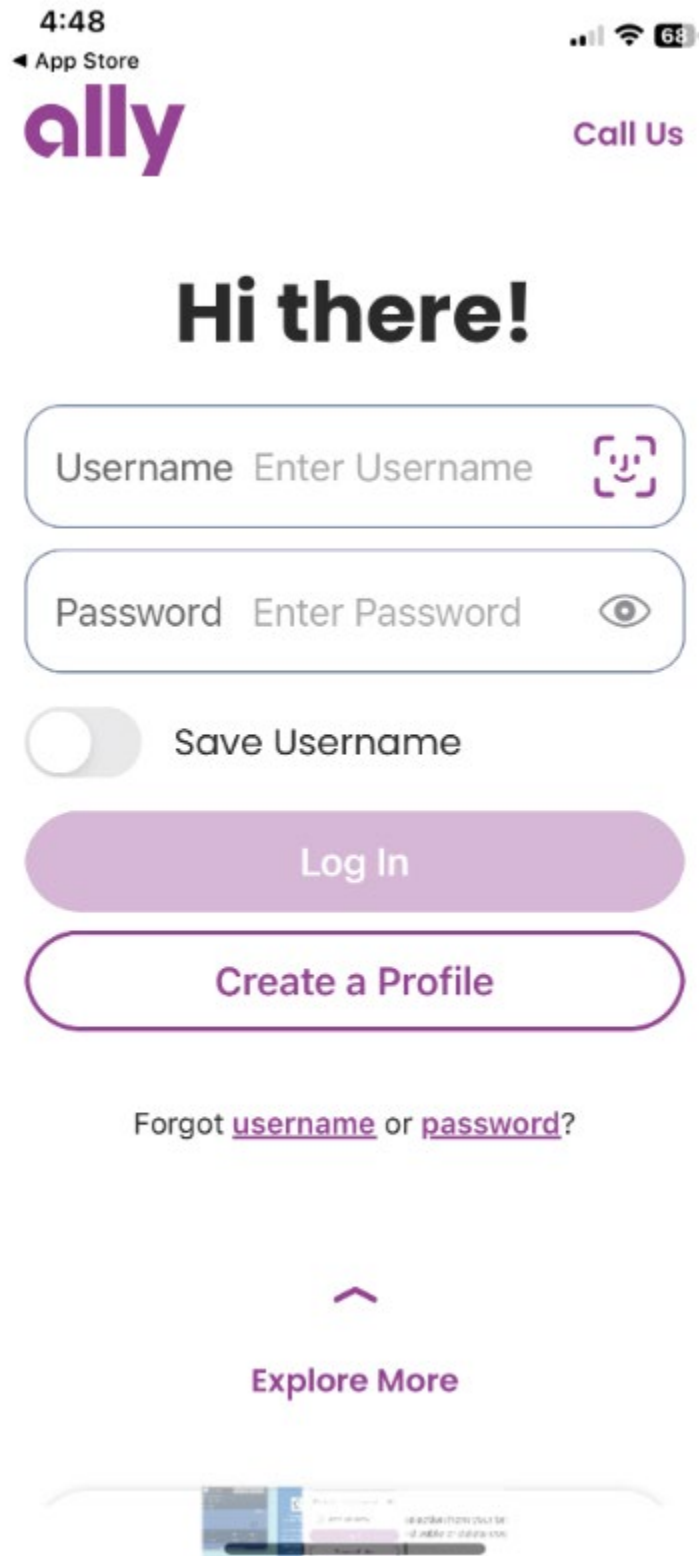
remote from the client machine for a current browsing session of the client machine; b. transmitting to the client machine the session identifier created in step a.; c. storing the session identifier transmitted in step b. within the client machine; d. verifying, on the client machine, that the client machine is authorized to access data maintained on the server computer; e. obtaining the session identifier stored in step c., and storing such session identifier within a storage table remote from the client machine if such client machine was verified in step d.; f. transmitting a request by the client machine for access to data maintained on the server computer, such request including the session identifier stored in step c.; g. comparing the session identifier transmitted in step f. with the session identifier stored in the storage table during step e. to determine whether the request for access transmitted in step f. is authorized; and h. permitting access by the client machine to the requested data maintained on the server computer if the comparison made in step g. shows that the request for access is authorized, and denying access by the client machine to the requested data maintained on the server computer if the comparison made in step g. shows that the request for access is not authorized.

24. The Accused Products practice a method of restricting access to data maintained on a server computer by an authorized client machine. For example, upon information and belief, on client machines running the Ally Financial Mobile Application variant for Apple iOS, one method by which an operator may sign in to access Ally Financial's "protected URLs," as an Ally Financial Account holder, is via Apple's Touch and Face ID (locally compared "biometrics").

Phones  	
Products & Rates	✓
Transfers	✓
Ally eCheck Deposit SM	✓
Savings Buckets & Boosters	✓
Spending Buckets	✓
Bill Pay	✓
Zelle [*]	✓
CD Management	✓
ATM Locator	✓
Ally Assist	✓
Biometric Verification (Optional)	✓

3

³ <https://www.ally.com/bank/online-banking/>



4

⁴ Screen shot of Ally Mobile Banking Application

25. The Accused Products further practice a method of creating a session identifier in a computer remote from the client machine for a current browsing session of the client machine. For example, upon information and belief, Ally Financial server computer(s) create one or more session identifiers, remote from the client machine, when a new user agent session on the client machine initially requests, via the HTTP protocol, an Ally Financial “protected URL.” For example, upon information and belief, an Ally Financial server creates a session identifier (e.g., a static or dynamic session ID, token, and/or certificate) upon successful access by a client device running the Ally Financial Mobile Application. Further, upon information and belief, when first launching the Ally Financial Mobile Application, a user agent requests Ally Financial URLs. In response to the request, one or more name-value pair(s) are created by the Ally Financial server(s).

26. The Accused Products further practice a method of transmitting to the client machine the session identifier created in step a. Upon information and belief, Ally Financial transmits the session identifier(s) to the client machine via the Internet. Session identifier(s) are transmitted by the Ally Financial HTTP server computer(s) to the client machine via one or more HTTP response headers and/or HTTP response bodies. For example, upon information and belief, an Ally Financial server transmits the session identifier (e.g., a static or dynamic session ID, token, and/or certificate) to a client machine (e.g., a phone running the Ally Financial Mobile App) upon initiating of the log-in process. Upon information and belief, this session identifier is stored in secure memory associated with the Ally Financial Mobile App, and used to identify the session by a client device (e.g., phone running the Ally Financial Mobile App) in subsequent communications and request/response processes with the Ally Financial server for the duration of a browsing session. Upon information and belief, each such communication includes at least one name-value pair, comprising of at least one session identifier.

27. The Accused Products further practice a method of storing the session identifier transmitted in step b. within the client machine. Upon information and belief, per instructions from Ally Financial servers and/or Ally Financial computer code, the web browser and/or application stores the session identifier(s) on the client machine. Upon information and belief, such instructions are transmitted in the form of code, automatically executed by the Ally Financial App, and/or by a browser operated based on computer instructions by the Ally Financial App. For example, upon information and belief, the Ally Financial Mobile App further stores the identifier in a client device (e.g., a phone), in secure memory associated with the application.

▼ Does Ally use cookies or other online technologies to collect information?

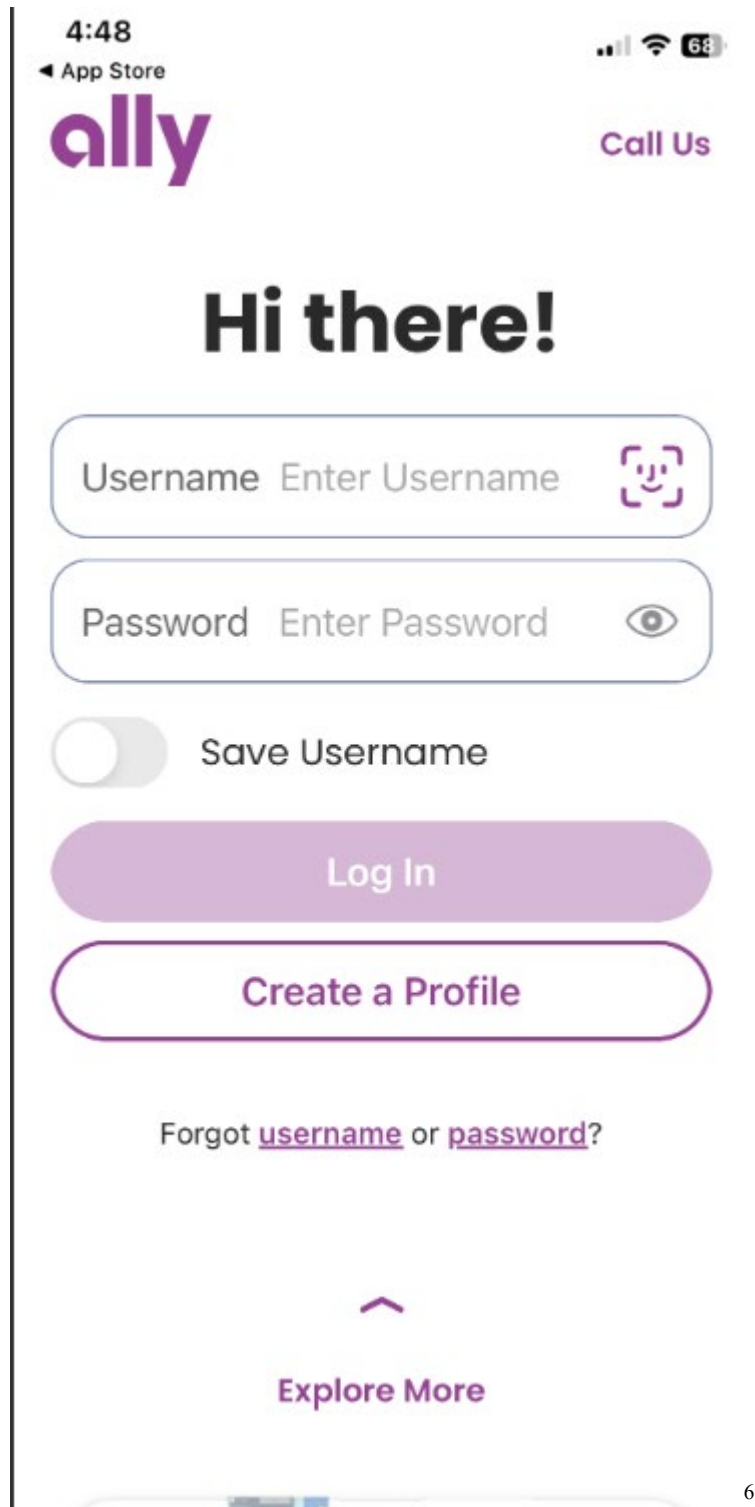
We use a variety of technologies, including cookies, to collect information about your online/mobile activity when you visit our website. Cookies are small text files that a website server stores on your computer or device. They're typically used to remember your account login preferences, monitor website traffic, provide customer support like live chat and help us better customize our site for your individual preferences.

We may also use Flash® objects (sometimes called "Local Shared Objects") as part of our online authentication to help us recognize your computer when you come back to our site. We do not use Flash objects for any online behavioral advertising purpose.

5



28. The Accused Products further practice a method of verifying, on the client machine, that the client machine is authorized to access data maintained on the server computer. Upon information and belief, when the client machine supports Apple Touch / Face ID, and the Ally Financial Mobile Application has been provisioned to sign in to Ally Financial online services via Touch / Face ID, Ally Financial computer code automatically prompts the operator to sign in via Touch / Face ID immediately after the application is launched. For example, upon information and belief, the Ally Financial Mobile Application verifies that a user is authorized to access data maintained on an Ally Financial server by locally authenticating and/or validating that its Session ID shows a user is logged in. For example, the Ally Financial Mobile App locally verifies that it is authorized to access data maintained on the Ally Financial servers by authenticating an operator's biometric information.

⁵ <https://www.ally.com/help/privacy-security>



6

⁶ Screen shot of Ally Mobile Banking Application

Phones  	
Products & Rates	✓
Transfers	✓
Ally eCheck Deposit SM	✓
Savings Buckets & Boosters	✓
Spending Buckets	✓
Bill Pay	✓
Zelle [*]	✓
CD Management	✓
ATM Locator	✓
Ally Assist	✓
Biometric Verification (Optional)	✓

7

29. The Accused Products further practice a method of obtaining the session identifier stored in step c., and storing such session identifier within a storage table remote from the client machine if such client machine was verified in step d. Upon information and belief, the Ally Financial Web Application is an extension or related to a remote Ally Financial storage table storing session identifier(s). For example, upon information and belief, once an operator has logged into the Ally Financial Mobile App using biometric authentication, the Ally Financial server system obtains the session identifier from the Ally Financial Mobile App client, e.g.,

⁷ <https://www.ally.com/bank/online-banking/>

through a request/response in which the client confirms local verification of biometric information. Upon information and belief, the Ally Financial Server then stores the session identifier in a table within secure memory associated with the server, where it is used to address transmission of data to the client.

30. The Accused Products further practice a method of transmitting a request by the client machine for access to data maintained on the server computer, such request including the session identifier stored in step c. Upon information and belief, per instructions from Ally Financial servers and/or Ally Financial computer code, upon successful sign in, the user agent is automatically redirected to the default Ally Financial Mobile Application page (an Ally Financial “Protected URL”) which invokes one or more HTTP requests. The HTTP request(s) are transmitted by the client machine and such request(s) include session identifier(s) to overcome limitations of the stateless HTTP protocol. For example, upon information and belief, the Ally Financial Mobile App running on a client machine (e.g., a phone) transmits requests for access to data maintained on the server computer (e.g., to Ally Financial brokerage and/or bank account data maintained on the Ally Financial server system). Upon information and belief, all request/response communications once the log-in process is initiated, including for such account data, include the session identifier.

31. The Accused Products further practice a method of comparing the session identifier transmitted in step f. with the session identifier stored in the storage table during step e. to determine whether the request for access transmitted in step f. is authorized. Upon information and belief, Ally Financial compares session identifier(s) remotely. For example, when session cookies (which store session identifiers(s)) are deleted from the client machine, the client machine is no longer logged in and no longer able to access Ally Financial “Protected URLs.” Furthermore, Ally

Financial indicates that “if you choose to disable or delete cookies, you may limit the functionality [Ally Financial] can provide when you visit [the Ally Financial] site.”⁸ Upon information and belief, the Ally Financial servers further compare the session identifier transmitted by an Ally Financial Mobile App with the corresponding identifier stored in a storage table to determine whether the request for access (e.g., to a brokerage and/or bank account) is authorized (e.g., whether the user logged in based on biometric information presented to the Ally Financial Mobile App).

▼ Can I disable or delete cookies?

Yes, you can disable cookies by making the appropriate selection from your browser options to inform you when cookies are set or to prevent cookies from being set. However, if you choose to disable or delete cookies, you may limit the functionality we can provide when you visit our site.

9

32. The Accused Products further practice a method of permitting access by the client machine to the requested data maintained on the server computer if the comparison made in step g. shows that the request for access is authorized, and denying access by the client machine to the requested data maintained on the server computer if the comparison made in step g. shows that the request for access is not authorized. Upon information and belief, if the client machine is signed in, access to data maintained on Ally Financial servers(s) is authorized by Ally Financial. If the client machine is not signed in, access to data maintained on Ally Financial servers(s) is denied by Ally Financial. For example, upon information and belief, the Ally Financial servers permit access by a client machine to the requested data maintained on the server computer (e.g., access to a brokerage and/or bank account by the Ally Financial Mobile App) if the comparison made in step g. shows that the request for access is authorized (e.g., that the user has logged in based on authentication of biometric information), or deny access (e.g., fail to return access to a bank

⁸ <https://www.ally.com/help/privacy-security>

⁹ <https://www.ally.com/help/privacy-security>

account information) if the comparison shows that the request is not authorized (e.g., a user's login was not successful).

33. For example, Ally Financial directly infringes at least claim 14 of the '262 Patent by making, using, offering to sell, selling, and/or importing into the United States products that comprise a computer program product tangibly embodied in an information carrier, the computer program product including instructions that, when executed, perform operations for restricting access to data maintained on a server computer, the method comprising: a. receiving a request from a client machine for access to data stored on a server; b. generating a password remote from the client machine, and providing the password to the client machine or to a user of the client machine, the password being derived from, and corresponding to, a client machine-specific identifier generated on the client machine; c. transmitting to the client machine instructions to regenerate the password and to verify, on the client machine, whether the client machine-specific identifier uniquely corresponds with the password generated at step b.; and d. allowing access to the data if the verification performed by step c. is true, and denying access to the data if the verification performed by step c. is false.

34. Each Accused Product comprises a computer program product tangibly embodied in an information carrier, the computer program product including instructions that, when executed, perform operations for restricting access to data maintained on a server computer, the method comprising the functionality of claim 14. For example, Ally Financial's servers supporting the Ally Financial mobile Application include a computer program product tangibly embodied in an information carrier (e.g., a software program running in memory) including instructions which, when executed, perform operations for restricting access to a user's account information via the

Ally Financial Mobile Application as recited below, e.g., by allowing access via biometric authentication.

35. Each Accused Product comprises a computer program product tangibly embodied in an information carrier, the computer program product including instructions that, when executed, performs receiving a request from a client machine for access to data stored on a server. For example, Ally Financial servers receive a request (e.g., an HTTP request) from a client machine (e.g., a smartphone running the Ally Financial Mobile Application) for access to data stored on a server (e.g., account information stored on a server) when the application is launched. For example, when first launching the Ally Financial Mobile App, upon information and belief, a user agent requests a protected URL associated with Ally Financial. Such requests are received by Ally Financial servers responsible for restricting access to account data. Upon information and belief, each such communication includes at least a name-value pair.

36. Each Accused Product comprises a computer program product tangibly embodied in an information carrier, the computer program product including instructions that, when executed, performs generating a password remote from the client machine, and providing the password to the client machine or to a user of the client machine, the password being derived from, and corresponding to, a client machine-specific identifier generated on the client machine. For example, the Ally Financial servers generate a password (e.g., a nonce, cryptographic key, public key, certificate, cryptogram, token, and/or other cryptographic material) derived from a client machine-specific identifier generated on the client machine (e.g., by applying a transform based on a seed value to a private key and/or device keys associated with or protected by the secure element of the device). The Ally Financial servers then provide that password to the client machine (e.g., by transmitting the password to a smartphone running the Ally Financial Mobile Application

via HTTP protocol). Upon information and belief, that password, is either stored inside, or wrapped in encryption provided by, a secure element/secure enclave of the mobile device running the Ally Financial Mobile Application. The seed value and algorithm are also stored inside or wrapped in encryption provided by that secure element/secure enclave.

37. Each Accused Product comprises a computer program product tangibly embodied in an information carrier, the computer program product including instructions that, when executed, performs transmitting to the client machine instructions to re-generate the password and to verify, on the client machine, whether the client machine-specific identifier uniquely corresponds with the password generated at step b. For example, upon information and belief, when biometric authentication is enabled on the Ally Financial Mobile App, the Ally Financial servers transmit instructions to re-generate the password (e.g., the seed value and algorithm that can be applied to the nonce, token, device key, public key, and/or key pair to generate a matching password and/or signed nonce), and to verify, on the client machine, whether the client machine-specific identifier uniquely corresponds with the password generated at step b. (e.g., by utilizing fingerprint, face, or iris recognition to authenticate a user, thereby granting access to the secure element-protected password, and applying the seed value and algorithm to the public key, nonce, signature, and/or key pair to verify that it matches the one transmitted by the server).

38. Each Accused Product comprises a computer program product tangibly embodied in an information carrier, the computer program product including instructions that, when executed, performs allowing access to the data if the verification performed by step c. is true, and denying access to the data if the verification performed by step c. is false. For example, if the sign in on the client machine is successful, access to data maintained on Ally Financial servers(s) is

authorized by Ally Financial. If the client machine is not signed in, access to data maintained on Ally Financial servers(s) is denied by Ally Financial.

39. Ally Financial indirectly infringes one or more claims of the '262 Patent by knowingly and intentionally inducing others, including Ally Financial customers and end-users of the Accused Products and products that include the Accused Products, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the Ally Financial Web and Mobile Applications.

40. Ally Financial indirectly infringes one or more claims of the '262 Patent, as provided by 35 U.S.C. § 271(b), by inducing infringement by others, such as Ally Financial's customers and end-users, in this District and elsewhere in the United States. For example, Ally Financial's customers and end-users directly infringe, either literally or under the doctrine of equivalents, through their use of the inventions claimed in the '262 Patent. Ally Financial induces this direct infringement through its affirmative acts of manufacturing, selling, distributing, and/or otherwise making available the Accused Products, and providing instructions, documentation, and other information to customers and end-users suggesting that they use the Accused Products in an infringing manner, including technical support, marketing, product manuals, advertisements, and online documentation. Because of Ally Financial's inducement, Ally Financial's customers and end-users use Accused Products in a way Ally Financial intends and directly infringe the '262 Patent. Ally Financial performs these affirmative acts with knowledge of the '262 Patent and with the intent, or willful blindness, that the induced acts directly infringe the '262 Patent.

41. Ally Financial indirectly infringes one or more claims of the '262 Patent, as provided by 35 U.S.C. § 271(c), by contributing to direct infringement by others, such as customers

and end-users, in this District and elsewhere in the United States. Ally Financial's affirmative acts of selling and offering to sell the Accused Products in this District and elsewhere in the United States and causing the Accused Products to be manufactured, used, sold and offered for sale contributes to others' use and manufacture of the Accused Products, such that the '262 Patent is directly infringed by others. The accused components within the Accused Products are material to the invention of the '262 Patent, are not staple articles or commodities of commerce, have no substantial non-infringing uses, and are known by Ally Financial to be especially made or adapted for use in the infringement of the '262 Patent. Ally Financial performs these affirmative acts with knowledge of the '262 Patent and with intent, or willful blindness, that they cause the direct infringement of the '262 Patent.

42. Ally Financial's infringement of the '262 Patent is willful, at least because it has knowingly and deliberately infringed the '262 Patent.

43. BrowserKey has suffered damages as a result of Defendant's direct and indirect infringement of the '262 Patent in an amount to be proved at trial.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury for all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, BrowserKey prays for relief against Ally Financial as follows:

- a. Entry of judgment declaring that Ally Financial has directly and/or indirectly infringed one or more claims of the '262 Patent;
- b. Entry of judgment declaring that Ally Financial's infringement of the '262 Patent is willful;
- c. An order awarding damages sufficient to compensate BrowserKey for Defendant's

infringement of the '262 Patent, but in no event less than a reasonable royalty, together with pre-judgment and post-judgment interest and costs;

d. Entry of judgment declaring that this case is exceptional and awarding BrowserKey its costs and reasonable attorneys' fees under 35 U.S.C. § 285;

e. An accounting for acts of infringement;

f. Such other equitable relief which may be requested and to which the Plaintiff is entitled; and

g. Such other and further relief as the Court deems just and proper.

Dated: April 28, 2025

Respectfully submitted,

/s/ Vincent J. Rubino, III

Alfred R. Fabricant
NY Bar No. 2219392
Email: ffabricant@fabricantllp.com
Peter Lambrianakos
NY Bar No. 2894392
Email: plambrianakos@fabricantllp.com
Vincent J. Rubino, III
NY Bar No. 4557435
Email: vrubino@fabricantllp.com
Jacob Ostling
NY Bar No. 5684824
Email: jostling@fabricantllp.com
FABRICANT LLP
411 Theodore Fremd Avenue
Suite 206 South
Rye, New York 10580
Telephone: (212) 257-5797
Facsimile: (212) 257-5796

Justin Kurt Truelove
State Bar No. 24013653
Email: kurt@truelovelawfirm.com
TRUELOVE LAW FIRM, PLLC
100 West Houston Street
Marshall, Texas 75670

Telephone: (903) 938-8321
Facsimile: (903) 215-8510

**ATTORNEYS FOR PLAINTIFF
BROWSERKEY LLC**